Come faccio a riconoscere se una email è falsa?

Autore : Giovanni Garro

Data: 18/01/2017

> ***Il decalogo con le regole fondamentali da seguire per non cadere nella trappola delle email di phishing e non farci rubare denaro e informazioni personali.***

Ogni giorno vengono **inviate decine di miliardi di email**. La posta elettronica è

diventato il mezzo di comunicazione più usato, e naturalmente è stato preso di mira anche dai soliti truffatori, persone con pochi scrupoli che sfruttano i nuovi strumenti digitali per raggirare le loro vittime.

A chi non è mai arrivata una email con la promessa di facili guadagni o per allertarci del furto dei dati bancari invitandoci a cliccare su un apposito link per cambiare le password? Si tratta quasi sempre di **messaggi falsi**, creati ad hoc per attirarci in trappola. Nonostante si tratti di un fenomeno molto diffuso e anche sul quale da più parti si cerchi di fare prevenzione, sono ancora molti a rimanere vittime di questi raggiri.

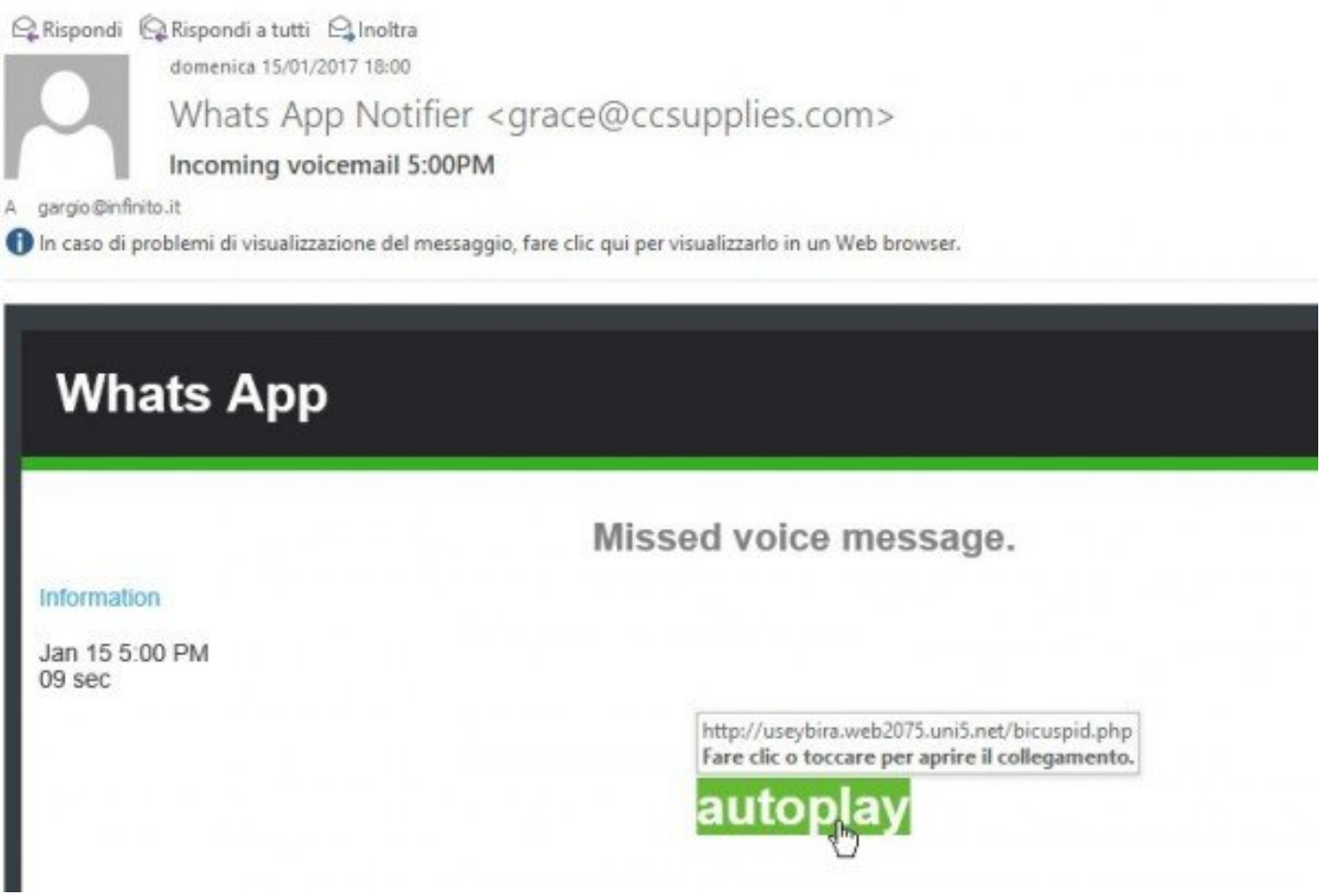
In gergo tecnico l'invio di email false viene identificato col termine **phishing**. Per capire la portata del phishing, basti dare un'occhiata alla propria casella di posta elettronica. Troveremo molto probabilmente un paio di **offerte vantaggiose**, un **messaggio dalla banca** che ci chiede di aggiornare i dati, qualche amico che ci invita a leggere un allegato. Siamo convinti che quei messaggi arrivano da qualche negozio online, dalla banca o da un amico, ma in realtà si tratta solo di email di phishing.

In pratica il **phishing è una tecnica utilizzata su larga scala** dai pirati informatici con la quale viene creata una email in modo che sembri arrivare da un mittente sicuro, come una istituzione pubblica, un negozio online o un amico. L'intento è quello di **indurre il destinatario a scaricare un virus o a inserire informazioni riservate su un sito web cui il pirata ha accesso**.

Come detto, si tratta di una tecnica applicata su larga scala: le **email fasulle vengono inviate a migliaia di destinatari nella speranza che qualcuno cada in trappola**. Un po' perché non si hanno le competenze per identificare quando il messaggio è falso, un po' perché le tecniche utilizzate sono sempre più intelligenti e personalizzate, sono tantissimi a rimanere vittime di questi raggiri.

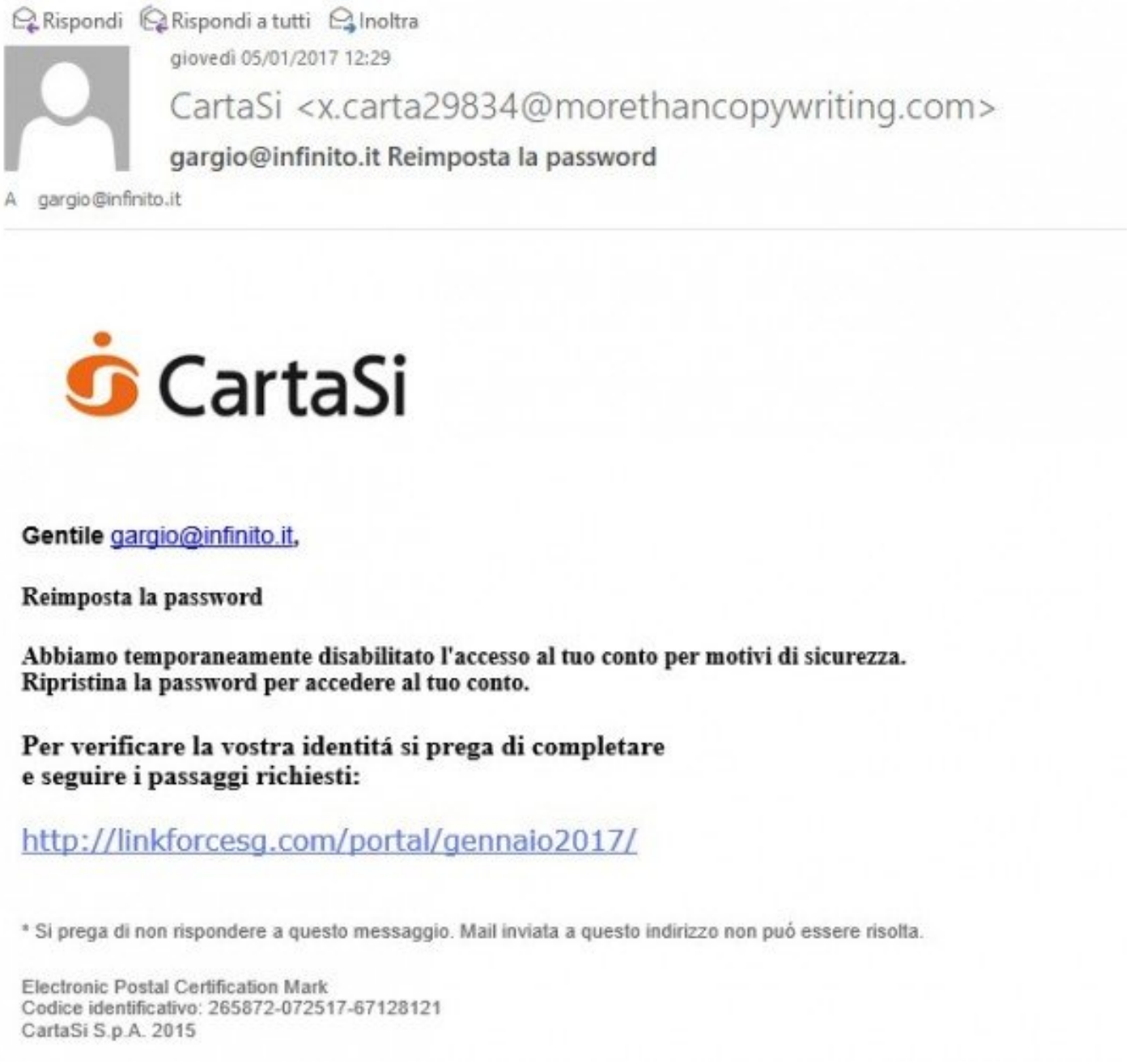
Ma come possiamo riconoscerle ed evitare di cadere in trappola? Ci sono una serie di elementi che ci possono aiutare a capire quando ci troviamo davanti una email di phishing. Ecco il **nostro decalogo** per non cadere in trappole ed evitare le truffe che viaggiano attraverso la posta elettronica.

1 Controllare la corrispondenza dei link presenti nella email. Un collegamento potrebbe essere indicato in un modo ma poi portare a un sito completamente diverso. Solitamente il client di posta consente di visualizzare l'url reale passando il puntatore del mouse sopra il link. Se non c'è corrispondenza, molto probabilmente si stratta di phishing.



2 L’indirizzo contiene un dominio ingannevole. I pirati utilizzano spesso la tecnica di creare sottodomini con i nomi di società attendibili e trarre in inganno la vittima. È bene sapere che il reale **dominio di un url** è quello che si trova all’estrema destra. Un url del tipo **info.apple.com** ha come dominio **apple.com**. Quello che sta a sinistra è un sottodominio, che appartiene ugualmente al dominio **apple.com**. L’hacker, invece, fa il contrario, ovvero crea un sottodominio usando il nome di una società legittima in modo da trarre in inganno la vittima. Ad esempio crea un url del tipo **apple.phishing.com**: la vittima così viene spinta a credere che si tratta di un messaggio inviato da **Apple** ma in realtà il dominio a inviarlo è **phishing.com**.

3 Nel messaggio sono richieste informazioni personali. Una banca o il gestore di telefonia di turno non chiederebbe mai per email il numero di conto, quello della carta di credito o la risposta a una domanda di sicurezza.



Rispondi Rispondi a tutti Inoltra

giovedì 05/01/2017 12:29

CartaSi <x.carta29834@morethancopywriting.com>

gargio@infinito.it Reimposta la password

A gargio@infinito.it

CartaSi

Gentile gargio@infinito.it,

Reimposta la password

Abbiamo temporaneamente disabilitato l'accesso al tuo conto per motivi di sicurezza.
Ripristina la password per accedere al tuo conto.

Per verificare la vostra identitá si prega di completare
e seguire i passaggi richiesti:

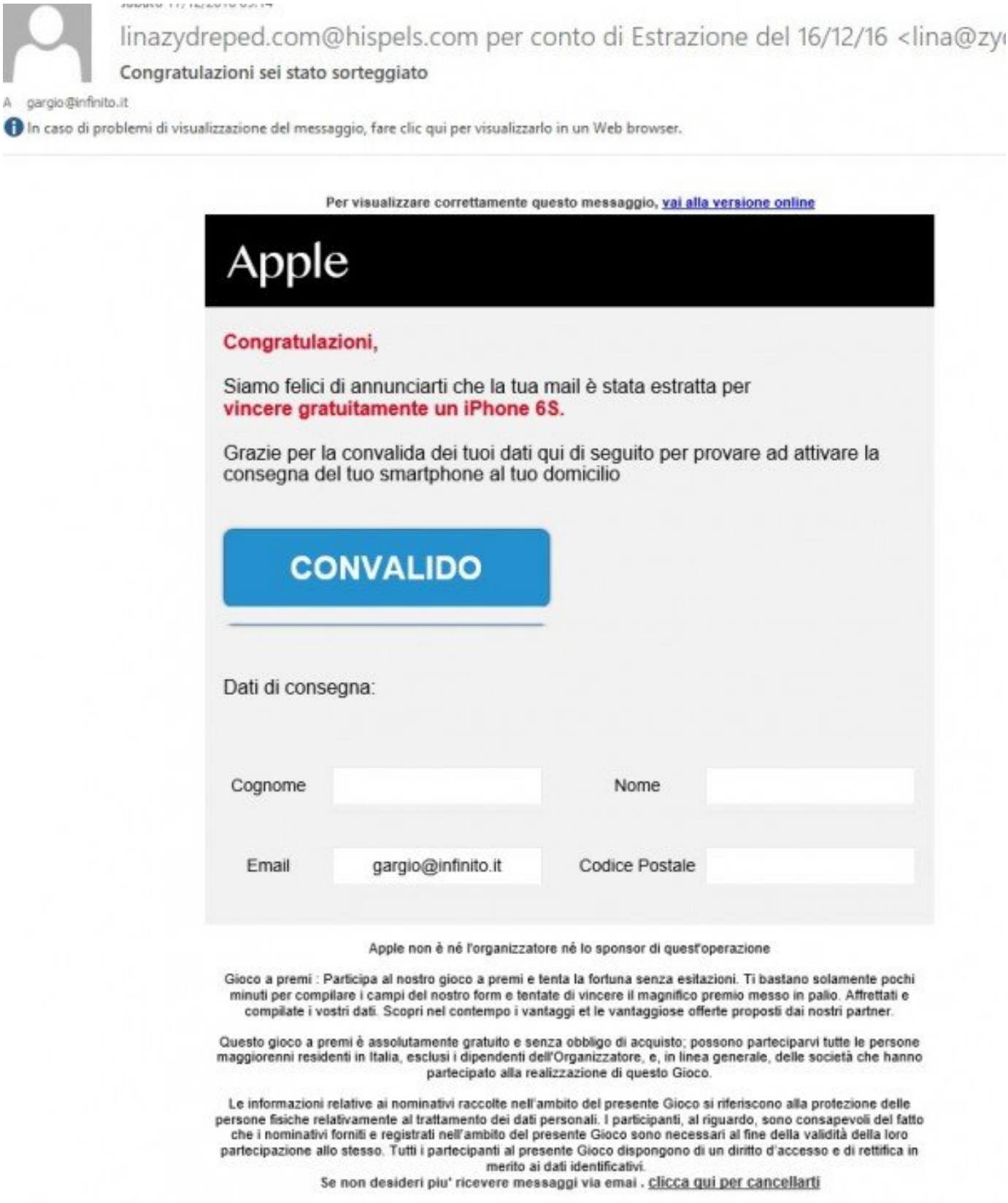
http://linkforcesg.com/portal/gennaio2017/

* Si prega di non rispondere a questo messaggio. Mail inviata a questo indirizzo non puó essere risolta.

Electronic Postal Certification Mark
Codice identificativo: 265872-072517-67128121
CartaSi S.p.A. 2015

4 Controllare se ci sono errori di ortografia e grammatica. Spesso le email di phishing sono generate da traduttori automatici ed inevitabilmente non sono in un italiano perfetto. Difficilmente una banca o un negozio commette errori del genere nelle loro comunicazioni.

5 Non siamo partecipanti al concorso. Se veniamo informati per email che abbiamo vinto a una lotteria o a un concorso a premi di cui non abbiamo acquistato alcun biglietto, possiamo essere sicuri che si tratta di una email di phishing.



linazydreped.com@hispels.com per conto di Estrazione del 16/12/16 <lina@zy

Congratulazioni sei stato sorteggiato

A gargio@infinito.it

In caso di problemi di visualizzazione del messaggio, fare clic qui per visualizzarlo in un Web browser.

Per visualizzare correttamente questo messaggio, vai alla versione online

Apple

Congratulazioni,

Siamo felici di annunciarti che la tua mail è stata estratta per **vincere gratuitamente un iPhone 6S.**

Grazie per la convalida dei tuoi dati qui di seguito per provare ad attivare la consegna del tuo smartphone al tuo domicilio

CONVALIDO

Dati di consegna:

Cognome | Nome

Email gargio@infinito.it | Codice Postale

Apple non è né l'organizzatore né lo sponsor di quest'operazione

Gioco a premi : Partecipa al nostro gioco a premi e tenta la fortuna senza esitazioni. Ti bastano solamente pochi minuti per compilare i campi del nostro form e tentate di vincere il magnifico premio messo in palio. Affrettati e compilate i vostri dati. Scopri nel contempo i vantaggi et le vantaggiose offerte proposti dai nostri partner.

Questo gioco a premi è assolutamente gratuito e senza obbligo di acquisto; possono parteciparvi tutte le persone maggiorenni residenti in Italia, esclusi i dipendenti dell'Organizzatore, e, in linea generale, delle società che hanno partecipato alla realizzazione di questo Gioco.

Le informazioni relative ai nominativi raccolte nell'ambito del presente Gioco si riferiscono alla protezione delle persone fisiche relativamente al trattamento dei dati personali. I participanti, al riguardo, sono consapevoli del fatto che i nominativi forniti e registrati nell'ambito del presente Gioco sono necessari al fine della validità della loro partecipazione allo stesso. Tutti i partecipanti al presente Gioco dispongono di un diritto d'accesso e di rettifica in merito ai dati identificativi.

Se non desideri piu' ricevere messaggi via emai , clicca qui per cancellarti

6 Se l'offerta è troppo bella per essere vera, probabilmente non lo è. Se riceviamo un messaggio da un mittente sconosciuto che ci promette facili guadagni o premi incredibili, quasi sicuramente è una truffa. Al Mondo nessuno regala nulla, non ci sono scorciatoie per diventare ricchi e comunque se avessimo vinto un premio, difficilmente verremmo contattati per email.


Rispondi Rispondi a tutti Inoltra

lunedì 16/01/2017 00:03

aldo@pagetti.it

Re: L'occasione! Restano a disposizione 91 posti.

A gargio@infinito.it

Caro gargio,

Io sono HR manager di una grande compagnia internazionale.
La nostra azienda è alla ricerca di collaboratori intraprendenti.
Il stipendio possibile da 2500 a 5000 euro al mese.

Se Le interessa nostra offerta - si prega di visitare il **Nostro Sito**

Con i migliori saluti,
HR Manager
Ufficio Internazionale

7 Viene chiesto di inviare denaro per coprire le spese. Uno degli obiettivi dei

truffatori è proprio quello di spillarci soldi. La richiesta di denaro solitamente non viene fatta subito, per non insospettire la vittima, ma prima o poi arriva, spesso con la scusa che la somma serve per coprire delle spese.

8 L'email contiene minacce irrealistiche. Molti hacker utilizzano la tecnica dell'intimidazione per convincere la vittima a fornirgli le informazioni personali. Se riceviamo una email dalla banca che ci avverte che il nostro conto verrà chiuso se non forniamo le informazioni richieste, probabile che si tratti di una falsa email: una banca non chiude un conto semplicemente attraverso una comunicazione per posta elettronica.

9 Ci vene notificata l'infrazione di una legge. Gli artisti del phishing spesso usano la tecnica di allarmare le vittime con email inviate da agenzie governative, polizia postale e forze dell'ordine facendo leva sul senso di rispetto della legge da parte dei cittadini onesti. Se avessimo violato qualche legge, difficilmente la cosa ci verrebbe comunicata attraverso una semplice email: si utilizzerebbero altri metodi molto più vicini al protocollo.

10 C’è qualcosa che non ci convince. Se riceviamo un messaggio che contiene qualcosa che ci insospettisce, è un buon segnale per dubitare della sua attendibilità. La regola fondamentale è sempre quella di adoperare il **buon senso** e vale anche e soprattutto per i messaggi di posta elettronica.